Win-Win sikkerhed i en digital verden
Få fordelene og undgå ulemperne ved RFID

Stephan J. Engberg

'Without changing our pattern of thought,
we will not be able to solve the problems we created
with our current patterns of thought'
Albert Einstein

Open Business Innovation

Making Privacy Default
.. because the alternative is not an option

Agenda

1. Problemerne i KODEKS kan løses teknisk
   - Ingen sikkerhed i RFID
   - RFID skal fjernes ved kassen
   - Der må ikke opsamles RFID-data i butikken
   - Tyverisikring (overvågningskameraerne)

2. Hvor ligger de tunge sikkerhedsproblemer?
   - Sikkerhedsparadigmet er forældet
   - Gatekeeperne

3. Hvad kan vi gøre?

Ingen sikkerhed i RFID

- Standard RFID har ingen sikkerhed - kan både kopieres, udsættes for man-in-the-middle Identitetstyveri, aflæses, trackes etc.

- Løsning #1 – ægthedsverificering / kopi-beskyttelse
  - Krav: Producent skal kunne verificere varen gennem hele værdikæden
  - Problem: RFID-tags har begrænset regnekraft og kapacitet
  - Vores Tekniske Løsning: Zero-Knowledge Device Authentication
    - En low-computational sikkerhedsprotokol, der ikke lækker identifiers
    - En stribe sikkerhedselementer inkl. f.eks. ikke-algoritmisk skiftende nøgler

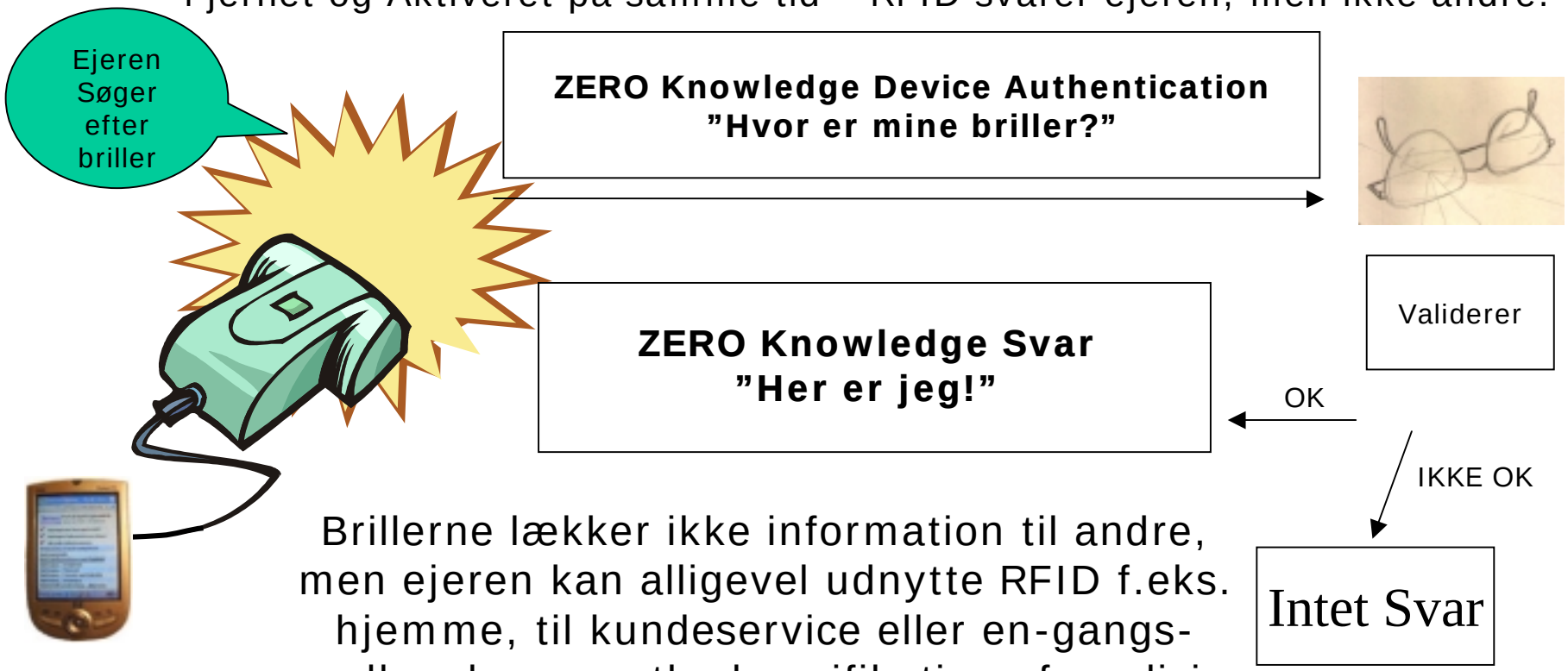
- Virker sådan
  - I butikken aflæses vare-nummer (f.eks. ePC) og sendes til producent
  - Producenten har en database med varenumre og shared secrets
  - Producent genererer og fremsender authentikerings-besked til RFID
  - Kun den pågældende RFID kan verificere beskeden og generere svar
  - Kun producenten kan verificere svaret (på forhånd som Hash(svar))

Kilde: http://www.obivision.com/Papers/PST2004_RFID_ed.pdf

Kodeks: RFID skal fjernes ved kassen!
Forbrugersikkerhed i praksis

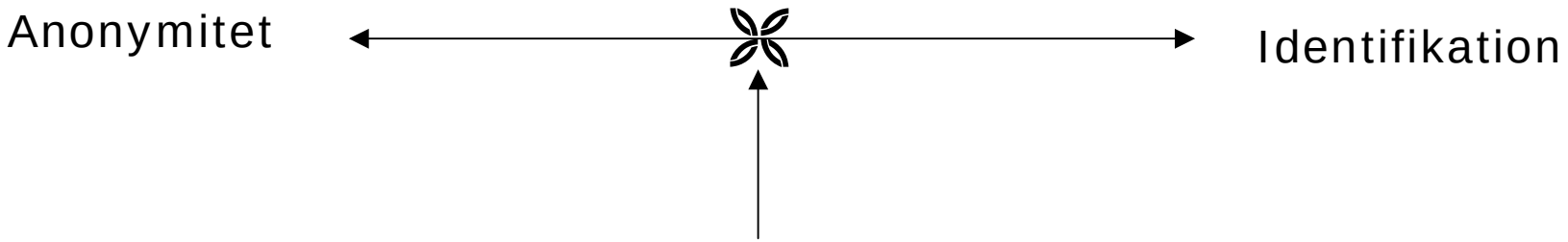
Problem: RFID skaber en masse sikkerhedsproblemer uden for butikken

Løsning # 2: RFID skifter til PRIVACY MODE i stedet for at blive slået ihjel
Forbrugeren overtager KONTROLLEN MED RFID – nøglen
Fjernet og Aktiveret på samme tid – RFID svarer ejeren, men ikke andre.



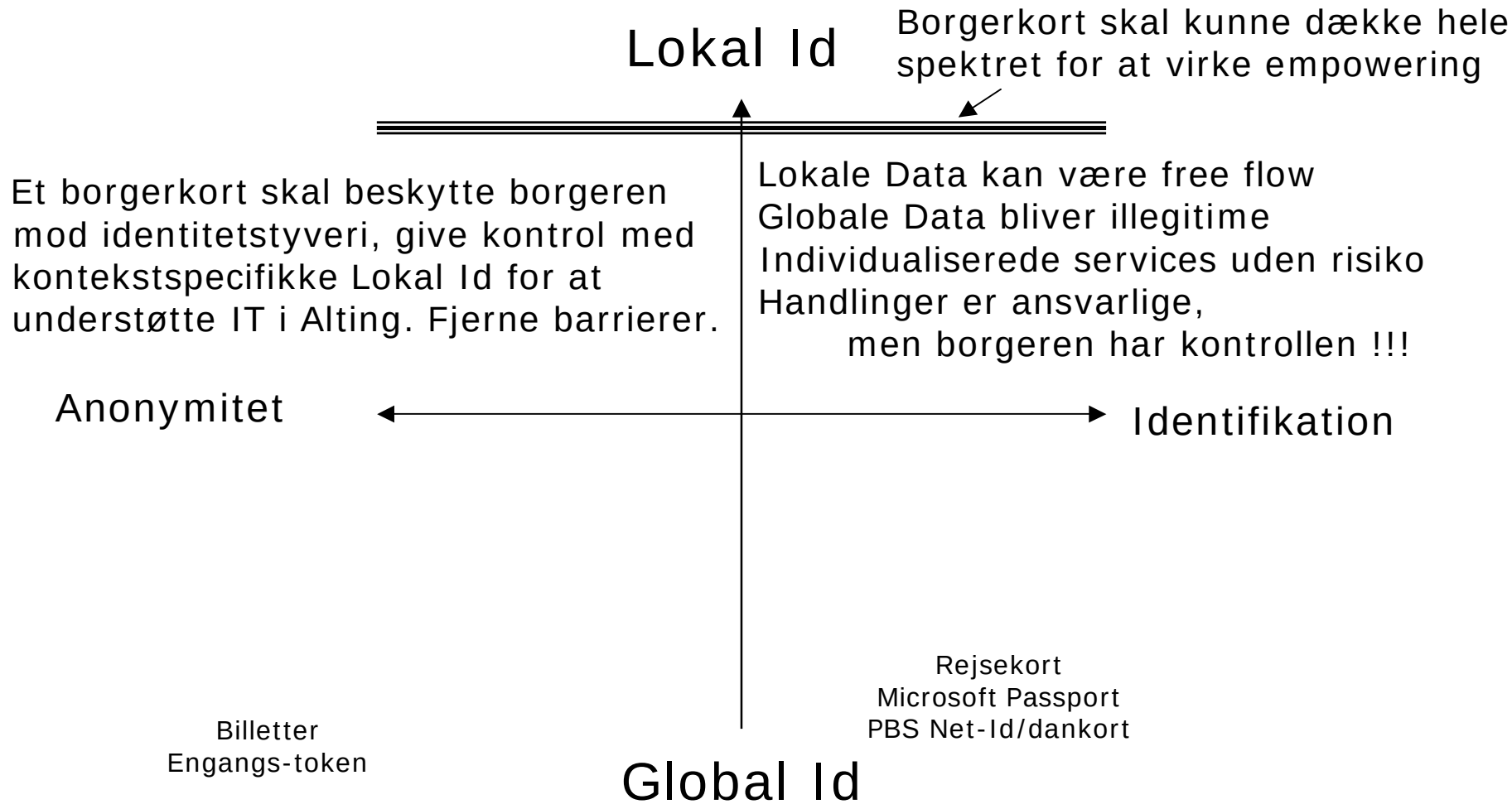
Brillerne lækker ikke information til andre, men ejeren kan alligevel udnytte RFID f.eks. hjemme, til kundeservice eller en-gangs-godkende en ægthedsverifikation af medicin mod EPJ umiddelbart før brug.

Det klassiske Problem



Et Borgerkort

skal give borgeren kontrollen !



Se f.eks. http://www.lawyersweekly.com.au/articles/23/0C020E23.asp?Type=56&Category=841

Kodeks: Butikkerne må ikke spore RFID

- Hvorfor må butikkerne ikke spore RFID-tags og bruge data?
  - Fordi betalingskort, mobiltelefoner, loyalitetskort og overvågningskameraer gør disse data til persondata og dermed misbrugbare, så tilliden eroderes !
  - DÅRLIGE Sikkerhedsprincipper (Global Id) ødelægger sikkerheden !!!

- Hvorfor underminerer vi sikkerheden i butikken !?
  - Butikker ønsker IKKE at ødelægge kunderelationen
  - Forbrugerne får IKKE flere services
  - Samfundet har ingen interesse i risikopræmien

- Løsning # 3 Borgerkort/Digitale Kontanthandler skaber vækst og sikkerhed
  - Ved at bruge LOKAL ID med Digital support af handel kan vi fjerne koblingen mellem RFID og Person, dvs. så sikkerhedsproblemerne aldrig opstår.

•F.eks. Betaling

- •Digitale Kontanter er fremtiden
- •Skaber ikke persondata – data er per definition sikre
- •Er selv-inkriminerende - beskytter mod falskmønteri
- •Er engangspenge – beskytter mod hvidvask

•F.eks. Kommunikation

- •Avancerede ”emailforward-adresser”
- •Mobiltelefoner – lokation Privacy
- •Kan gøres anonyme – eller næsten enhver balance
- •Ny hver gang
- •Forbrugeren kan selv koble flere transaktioner

Se http://www.obivision.com/papers/privacyauthentication.pdf

Tyverisikring
Styr på overvågningskameraer

- Løsning # 4 Erstat overvågningskameraer med mere sikker teknologi baseret på RFID og Lokal Id.

- RFID kan varesikre VAREN uden at overvåge Forbrugeren.
  - Kameraer blokeres FYSISK, så alle ved selvsyn kan se at der ikke filmes.
  - Kameraer/alarm slås FØRST til ved forsøg på tyveri eller på at fjerne tags.
  - Sporing af tags i butikken bruges til kundeservices.

- Sikre Borgerkort med LOKAL ID kan sikre TRANSAKTIONEN
  - Man ”logger ind” med engangs-id (I bankerne sker det alligevel)
  - Hvis kunden IKKE ”logger ind”, så aktiveres kameraer / evt. tavs alarm.
  - Kan designes så NØGLERNE slettes automatisk (f.eks. efter 24 timer)

Hvorfor har man så travlt med overvågningskameraer ?
De gør hverken samfundet rigere eller tryggere

F. eks. Teknologirådet: http://www.tekno.dk/subpage.php3?article=1077&toppic=kategori2&language=dk

Win-Win Sikkerhed

Få fordelene ved RFID uden ulemperne

Hvad har vi opnået / demonstreret ?

Forbrugerne opretholder kontrollen med egne data
Butikkerne får flere data og bedre kunderelationer

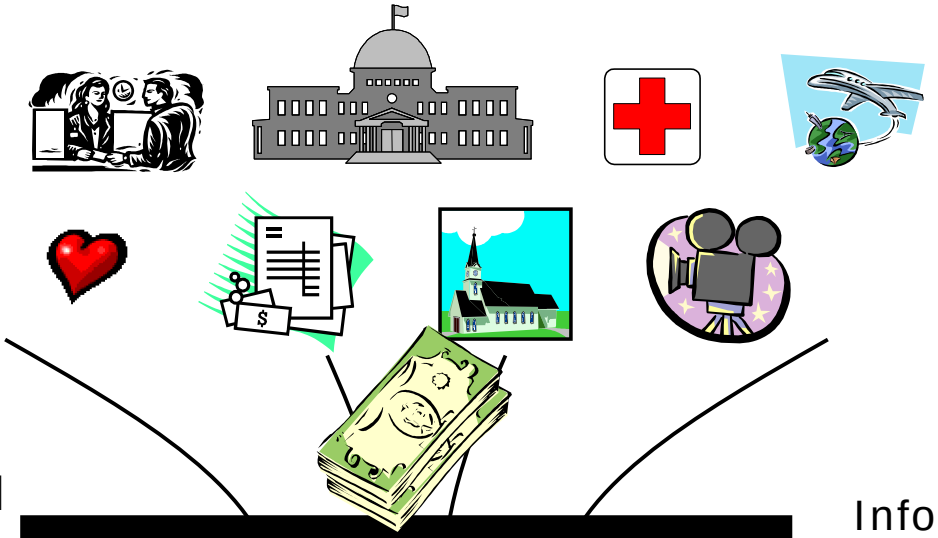
- Anti-kopisikring og forbrugersikkerhed i hele værdikæden
- Levende RFID kan bruges til IT-i-Alting
- Butikkerne kan spore varene med indbygget tyverisikring
- Forbrugernes shopping proces kan understøttes
- Overvågningskameraerne tændes kun ved misbrug

Intellectuals solve problems; geniuses prevent them.
--Albert Einstein

KODEKS er kun nødvendigt fordi markedet IKKE virker !!

Gatekeeperne ønsker kontrol med forbrugerne
Er vi ved at genindføre ”Stavnsbåndet”?

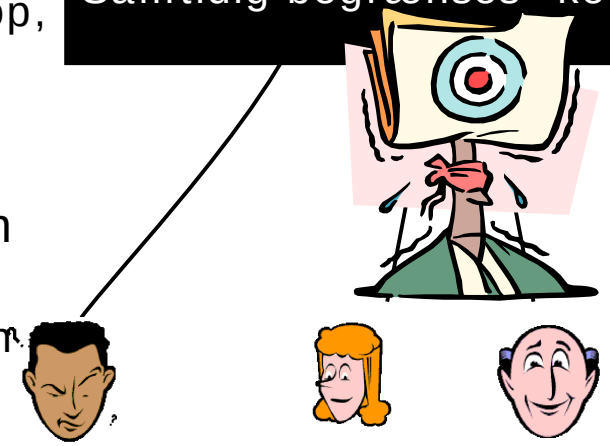
Leverandører bliver
underleverandører
og (af)presses på pris



Baseres på lokalt monopol
af en ressource/device:
MS Passport, PBS/Dankort,
Net-Id, mobiltelefon, set-top,
Rejsekort etc.

Konkurrencen reduceres
Samtidig begrænses ”konvergens”

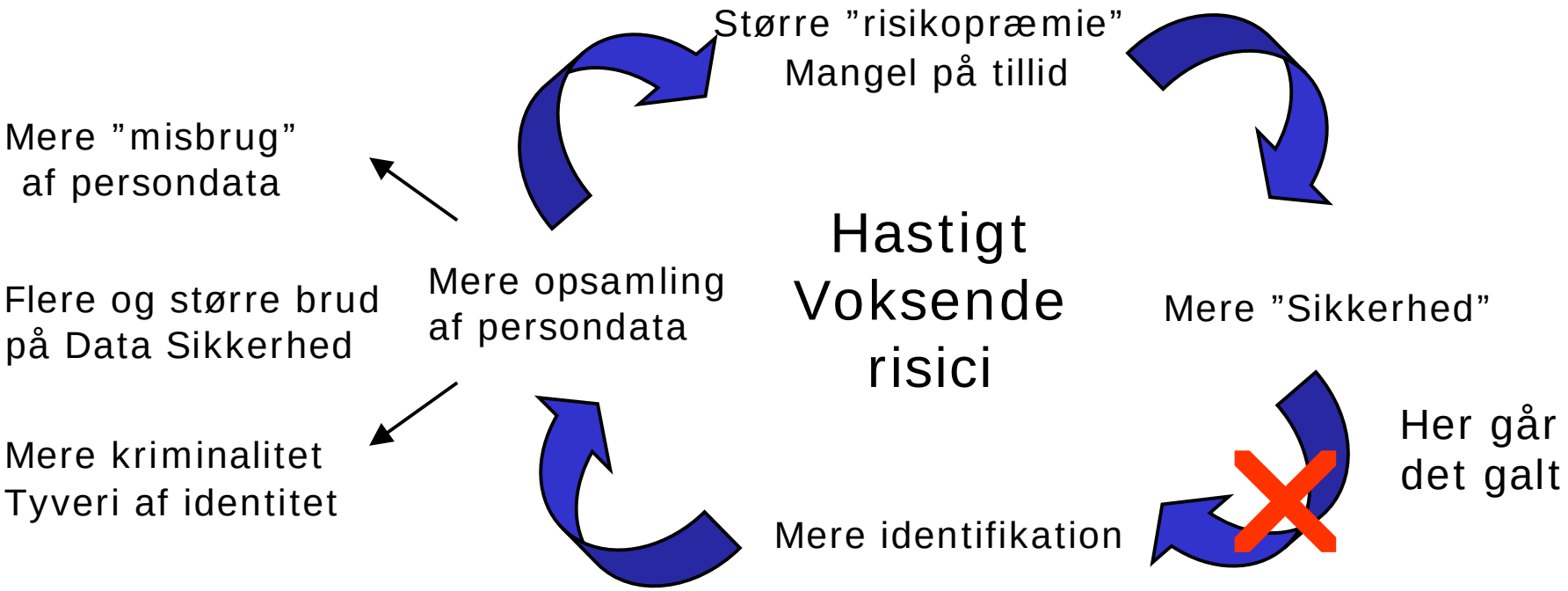
Infomediary
Gatekeepere
Id-Brokere
Portaler



Individet mister kontrollen
og sikkerheden eroderes
Identitetstyveri, koncentration
og sekundær datamisbrug

HOVEDPROBLEM:
NØGLERNE
TIL DIT LIV
”EJES”
AF GATEKEEPER

Sikkerhedens Onde Cirkel



Mere falsk sikkerhed
- Tyveri af identitet

Singapore om Pas m. Biometri*
”We will have more fake passports”

Mere Central kontrol

Mere overvågning
E.g. Mobil m. kamera
- Industrispionage
- Intimsfæren

http://www.prime-project.eu.org/public/prime_products/papers/studies/IDTheftFIN.pdf
*http://www.itsc.org.sg/events/cpitc_seminar_oct03/Tough_Problems_Facing_Biometric_Passports.pdf
http://www.jrc.es/home/publications/publication.cfm?pub=687

Hvad kan vi gøre?

- Persondataregulering – Ejerskab af egne data
  - Samtykke eroderes
    - –> Grundlovens princip om Ejendomsret til egne data
  - Stil krav til teknologien – eller bliver den deterministisk
  - Teknisk sikkerhed kan styrke Jura – Lokal Id
- Marked – Giv Forbrugerne Kontrollen/Empower
  - Vi kan skabe den digitalt understøttede kontanthandel
  - Damage control – Lokale data er sikre og skaber tryghed
  - Fra push til demand-pull – Brugerdreven innovation
- Teknologi – Fokus på Borgernes sikkerhed
  - Design ALTID med Lokal Id – specielt server-side
  - Fælles Borgerkort – must-carry af hensyn til konvergens
  - Privacy Impact Assesments - fokus på forebyggelse

Effektiviserer bedre og hurtigere !!!

Gartner Group
Om privatlivets fremtid

”Om 10 år vil anonymitet og beskyttelse af Privatsfæren være begreber næsten uden betydning.”

“ (sje: RFID og langdistance trådløs kommunikation) vil skabe et samfund, hvor alle er online konstant, og en lang række informationer lagres om den enkelte.”

“Information om hvem vi er, hvor vi er og hvor vi har været, vil ikke længere være en privat sag, men derimod informationer, som til enhver tid kan genskabes”

”De forskellige privatsfærer smelter sammen”

Gartner Group, April 2004, http://www.jp.dk/itogc/artikel:aid=2374038/

Den digitale verden

Teknologien kontrollerer Mennesket !

eller

Mennesket kontrollerer Teknologien !

Systemkontrol:

Vi er ALTID er identificeret, overvåget og registreret i databaser udenfor vores kontrol.

Personlig frihed:

Vi bruger teknologien til at give individet kontrollen med persondata i databaserne.

Kan den digitale verden overhovedet fungere, hvis mennesket føler sig eller er sat uden for kontrol?